UMA telecon 2010-11-18

UMA telecon 2010-11-18

• Date and Time
• Agenda
• Attendees
• Minutes
  • New AI summary
  • Roll call
  • Approve minutes of 2010-10-28, 2010-11-01, and 2010-11-11 meetings
  • Meeting schedule for the rest of 2010 (see bottom of page)
  • Action item review
  • Brief updates from the wider UMA world
  • Brainstorm and record outstanding resource registration issues (no discussion) - full proposal, JSON
  • Review latest trusted claims proposal
  • Ensure new user stories are captured
  • Line up next set of spec issue priorities
• Next Meetings

Date and Time

• WG telecon on Thursday, 18 Nov 2010, at 9-10:30am PT (time chart)
  • Skype line "C": +9900827042954214
  • US: +1-201-783-9022 | Room Code: 295-4214

Agenda

• Roll call
  • New participant introductions
• Approve minutes of 2010-10-28, 2010-11-01, and 2010-11-11 meetings
• Meeting schedule for the rest of 2010 (see bottom of page)
• Action item review
• Brief updates from the wider UMA world
• Brainstorm and record outstanding resource registration issues (no discussion) - full proposal, JSON
  • Need to define the user redirection piece?
  • What else?
• Review latest trusted claims proposal
  • See also further explanation/links
• Ensure new user stories are captured
  • Stories from IIW F2F
  • Transitive access
  • Backup service
• Line up next set of spec issue priorities
  • Claims 2.0 (plus other bootstrap claims definitions?)
  • Dynamic registration
  • Other?
• AOB

Attendees

As of 15 Nov 2010, quorum is 8 of 14.

Attending:

1. Adams, Trent
2. Bryan, Paul
3. Catalano, Domenico
4. D'Agostino, Salvatore
5. Fletcher, George
6. Maler, Eve
7. Morrow, Susan
8. Scholz, Christian

Non-voting participants:

• Alam
• Kevin Cox
• Mark Lizar
• Mike Seilnacht
• Anna Ticktin (staff)

Regrets:

• Maciej Machulak
Minutes

New AI summary

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Ope</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-11-18</td>
<td>Eve</td>
<td>Ope</td>
<td>Work with staff to ensure that the modified UMA meeting schedule is put online.</td>
</tr>
<tr>
<td>2010-11-18</td>
<td>Eve</td>
<td>Ope</td>
<td>Figure out who will speak at the ITU-T meeting.</td>
</tr>
<tr>
<td>2010-11-18</td>
<td>Domenico, Sal</td>
<td>Ope</td>
<td>Explore turning the trusted claims UX and writeup into draft spec text.</td>
</tr>
<tr>
<td>2010-11-18</td>
<td>Eve</td>
<td>Ope</td>
<td>Capture new user stories in the wiki.</td>
</tr>
</tbody>
</table>

Roll call

Quorum was reached.

Susan is head of R&D at Avoco Secure. They are keeping an eye on standards that are relevant to their work. Avoco specializes in security software, document security, and data security, and they have a fully cloud-based identity selector.

Approve minutes of 2010-10-28, 2010-11-01, and 2010-11-11 meetings

Minutes of 2010-10-28, 2010-11-01, and 2010-11-11 meetings APPROVED.

Meeting schedule for the rest of 2010 (see bottom of page)

Eve has proposed a few extra meetings:

- Focus call on Wednesday, 24 Nov 2010, at 9-10:30am PT (time chart) ?? – YES.
- WG telecon on Wednesday, 22 Dec 2010, at 9-10:30am PT (time chart) ?? – presumably YES. We'll check closer to the time.

Action item review

- 2010-08-26-6 Eve Open Ping Denise Tayloe of Privo to see if she has interest in taking custodian scenario forward. Pending Scenario doc edits. Let's drop this for now.
- 2010-10-07-2 Sal, Domenico Closed Propose the next version of the trusted claims solution, making appropriate simplifying assumptions.
- 2010-11-01-1 Alan Closed Write up backup service/copy service use case, with reference to requester delegate scenario.
- 2010-11-01-2 George Open Write up "problem B" as a user experience description that can be turned into a user story. He hopes to do it by next week.
- 2010-11-01-2 Eve Open Put the public-private continuum language and diagram into the Lexicon. She hopes to do it by next week.

Brief updates from the wider UMA world

- UMA presentation on Dec 10 in Geneva: Sampo, Juan, Eve?

It's also an option for Joni to present, as she'll be present. Perhaps it's best for Joni+Eve to present.

Brainstorm and record outstanding resource registration issues (no discussion) - full proposal, JSON

George describes the discussion held last week. It involved the boxcarring discussion, expectations around what information the AM needs to know, and the possibility that the AM could apply default policies. Last week it was generally agreed that the host can manage its own understanding about how resources are grouped, and the AM would only know that the user wants to protect "this string".

The JSON that was presented would support this model. Then the AM is just assigning policies to the string that it got from the host, and the host alone knows what sets of resources are associated with that string.

Since Problem B was all about the user protecting resources without leaving the host, this model could satisfy this requirement pretty easily since the host alone knows about "resources" vs. registered strings. Paul further comments that these strings could be URIs; nothing in the format prevents it.

The host could then determine the circumstances and times at which it pushes registration information to the AM. Do we need to keep the redirection piece that's defined in the current proposal? It seems so, since we need to satisfy the "sharing" use case, which involves mapping real policy to the groupings. The host might very well present a grouping as "for family", which gives the illusion of setting policy – or perhaps, more accurately said, prepares the ground more thoroughly for policy to be mapped.

Eve asks: How would this impact the scope strings' traversal through the stages of the protocol, particularly the point where the requester has to ask the AM for a particular access token for a particular scope of access? We think it might work, but it needs to be integrated into the full spec to see what happens. Eve suspects that, by now, we want to incorporate this directly into the core spec.

Would the scope strings and display names ever be exposed to requesting users? This would bring up the question of the natural language(s) in which the display name is provided.

The question of "protecting without sharing" still involves mapping a policy (at some point, either by default or at the time of putting the resource under protection) that says "don't share this with anyone". So the analysis of this point at the IIW F2F wasn't quite right.
Let's focus on integrating new spec text in the Wednesday focus call next week.

**Review latest trusted claims proposal**

- See also further explanation/links

Domenico has just sent a V08 UX, and a new writeup.

Domenico explains that you could use NASCAR-like interfaces to associate IdPs (“subject registration”) and sources of other trusted claims (“claims hosts”) with your CopMonkey AM account. The distinction between the two is largely based on UX vs. protocol differences, since a claim about your GMail identifier from Google could look very similar to a claim about your employment status from MyCompany.

For each claims host, the wireframes show how you can manage policies for sharing them (the radio buttons on “Basic Attributes”), and how you can add new individual trusted claims.

When Bob is at MyPhoto.com and enters the link of Alice’s protected photo, and subsequently gets a 401 with the location of AM1, his requester goes to AM1, which tells him/his requester that they need to have a proof of email. Then his requester discovers (how?) AM2, which is acting as a sort of “claims broker” (how?). Perhaps we can bypass the fancy auto-discovery piece if Bob can tell MyPhoto which AM to use, e.g. if he’s already protecting his own resources at MyPhoto with his AM.

Does MyPhoto (Bob’s requester) actually “handle”/touch the claim, or does it just arrange for Alice’s AM to go get the claim from Bob’s claim host directly? The latter would allow us to use “vanilla UMA” as much as possible, and would seem to have an easier security proposition, since you don’t have to protect the claim against MyPhoto tampering. Then again, Alice’s AM would have to be control of Bob’s browser in order to kick off such a flow.

The standardization of claim types is something we should ideally not have to worry about, but we do need a basic solution for it. We have the bare bones of a solution in the Claims 2.0 spec, with the notion of a claim type URI, and of course there are claims catalogs in existence.

The proposal here accommodates the notion that any one claim can be associated with a particular level of assurance.

We need to solve for getting claims from multiple claims hosts to satisfy any one policy.

Eve would like to explore a next step of turning the UX and writeup into draft spec text.

**Ensure new user stories are captured**

- Stories from IIW F2F
- Transitive access
- Backup service

**Line up next set of spec issue priorities**

- Claims 2.0 (plus other bootstrap claims definitions?)
- Dynamic registration
- Other?

We will want to check out the new JSON token work being done on the OAuth side to see if it can be applied to our Claims 2.0 work.

We’ll have to catch up with Maciej on the dynamic registration status next time.

**Next Meetings**

- Focus call on Wednesday, 24 Nov 2010, at 9-10:30am PT (time chart)
- WG telecon on Thursday, 2 Dec 2010, at 9-10:30am PT (time chart)
- WG telecon on Thursday, 9 Dec 2010, at 9-10:30am PT (time chart)
- WG telecon on Thursday, 16 Dec 2010, at 9-10:30am PT (time chart)
- WG telecon on Wednesday, 22 Dec 2010, at 9-10:30am PT (time chart)